Botnets, redes organizadas para el crimen

Autor: Lic. Cristian Borghello,Technical & Educational de Eset para Latinoamérica

Fecha: Martes 27 de febrero del 2007

Eset, LLC 1172 Orange Ave., Coronado, California 92118, USA
phone: (619) 437 – 7037, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

El poder de Skynet (la súper computadora de la película Terminator) en el dedo de un terrorista digital. Si quisiéramos exagerar (o quizá no) y ponernos paranoicos al extremo, quizás esa sería la forma de pensar este artículo. ¿Puede una sola persona dominar el poder necesario para hacer caer sitios y redes completas con sólo un clic?

Por otro lado, si se piensa que se envían 100 billones de mensajes de correo al día es sencillo adivinar por qué hay tanta basura virtual dando vueltas.

Y ya que comenzamos con los números, por qué no decir que el 80% (o más) del correo actual es considerado spam y el 80% (o más) del mismo es generado por los mismos usuarios que lo reciben.

¿Cómo? Según algunos expertos[1], los usuarios generamos el poder computacional distribuido suficiente para controlar el 25% de Internet con un clic y además generar el tráfico de spam del que nos quejamos.

¿Cómo? La respuesta es sencilla y sólo requiere de una palabra: botnets

Para no reinventar definiciones ya establecidas según la Wikipedia, un zombi[2] es, originalmente, una figura legendaria propia de las regiones donde se practica el culto vudú. Es un muerto resucitado por medios mágicos por un hechicero para convertirlo en su esclavo. Por extensión, ha pasado a la literatura fantástica como sinónimo de muerto viviente y al lenguaje común para designar en sentido figurado a quien hace las cosas mecánicamente como si estuviera privado de voluntad.

Si se toma la última parte de la definición estaremos entrando de lleno en nuestro informe.

Un bot (proveniente de robot) es un programa informático cuya función fundamental es realizar tareas, generalmente repetitivas y automáticas, simulando al ser humano.

Son utilizados por aplicaciones y sistemas tan dispares como pueden ser los canales de Chat, automatización de instalaciones, la misma enciclopedia Wikipedia, juegos en línea, programas de administración remota y tantas otras aplicaciones. Dependiendo del contexto de uso, su nombre puede variar (bot, borg, crpg) pero el concepto de realización de tareas automáticas se mantiene.

---

[1] Criminals 'may overwhelm the web'
http://news.bbc.co.uk/1/hi/business/6298641.stm

[2] Zombie
http://es.wikipedia.org/wiki/Zombie

El poder de la distribución

SETI@home[3] es un experimento científico de la Universidad de Berkeley que utiliza ordenadores conectados a Internet para la búsqueda de inteligencia extraterrestre. Cualquier usuario puede participar en forma voluntaria instalando un programa en su equipo y "donando" tiempo ocioso del mismo para el cálculo de datos recibidos de los distintos radiotelescopios internacionales.

En forma similar BOINC[4] es un proyecto científico para crear una red distribuida con distintos objetivos benéficos y distributed.net[5] es un proyecto destinado a probar la fortaleza de distintos algoritmos de cifrado actuales.

El poder del cómputo distribuido[6] radica en que pueden utilizarse sistemas heterogéneos (Win*, *nix, BSD, Mac, etc) para atacar problemas complejos que no pueden resolverse en las supercomputadoras actuales en un tiempo razonable.

Sin ir más lejos, este es el principio de las redes P2P[7] en donde no existen servidores, sino que todos los clientes (nodos) tienen el mismo nivel de privilegio dentro de la red. Además, este tipo de cómputo permite que los sistemas sean escalables (la cantidad de nodos es, en teoría, ilimitada) y tolerantes a fallos (si uno de los nodos falla el mismo puede ser inmediatamente reemplazado por otro).

Tal y como distributed.net mismo dice, el poder del cómputo distribuido les ha permitido "llegar a ser el equivalente a más de 160.000 computadoras PII 266 MHz trabajando 24 horas al día, 7 días a la semana, 365 días al año".

---

[3] Sitio de SETI@home
http://setiathome.berkeley.edu/index.php

[4] BOINC (Berkeley Open Infrastructure for Network Computing)
http://boinc.berkeley.edu/

[5] Sitio de Distributed.net
http://distributed.net/

[6] Computación distribuida
http://es.wikipedia.org/wiki/Computaci%C3%B3n_distribuida

[7] Redes P2P (Peer to Peer – Redes de Pares)
http://es.wikipedia.org/wiki/P2p

Pero, ¿cuál es el problema complejo a resolver en este caso? Como se menciona al comienzo, el envío de spam y el ataque combinado a sitios webs, generalmente conocido como DDoS[8].

Origen de las botnets

Cuando el negocio del spam y los problemas asociados, como la distribución de malware y phishing, lograron alcanzar niveles de rentabilidad suficiente para los cyber-delicuentes actuales, los mismos tenían un problema importante entre manos.

Los servidores vulnerables secuestrados hasta el momento y aquellos que se descubrían a diario, ya no eran suficientes para los objetivos de estas personas. El problema entonces, radicaba en lograr la distribución de más correos para llegar a más usuarios y así maximizar sus ganancias. La solución llegó de la mano del poder de cómputo distribuido.

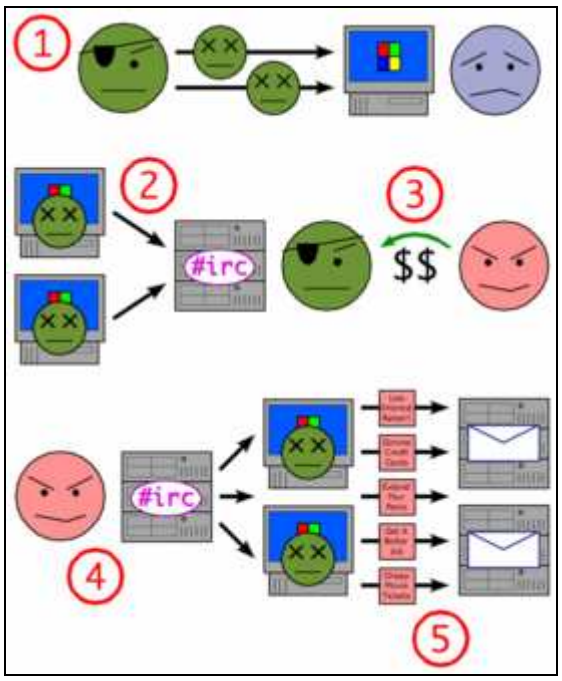
Pero, ¿cómo aprovechar el equipo del usuario para que él mismo "done" su sistema con fines delictivos? La solución, al igual que en los casos mencionados SETI y otros proyectos, es instalar un cliente en el equipo del usuario para que el mismo funcione de nexo con el malhechor.

La forma de instalar estos programas clientes es crear troyanos/gusanos que infecten al usuario, haciendo que su equipo interactúe en la red que se forma y sin que el usuario se entere de lo sucedido. Así, el equipo infectado se acaba de convertir en un zombi o robot haciendo cosas mecánicamente como si estuviera privado de voluntad.

El conjunto de equipos (usuarios) infectados trabajando en red recibe el nombre de botnet.

[8] DDOS (Distributed Denial Of Service Attack - Ataque de Denegación de Servicio Distribuido)
http://es.wikipedia.org/wiki/DDoS
http://es.wikipedia.org/wiki/DoS

El gráfico[9] disponible en la Wikipedia explica en forma concisa el funcionamiento descrito:



1. El operador de la botnet manda virus/gusanos/etc a los usuarios.
2. Las PCs entran en el IRC o se usa otro medio de comunicación.
3. El spammer le compra acceso al operador de la Botnet.
4. El Spammer manda instrucciones vía un servidor de IRC u otro canal a las PC infectadas.
5. Causando que éstos envíen Spam al los servidores de correo.

[9] Botnets
http://es.wikipedia.org/wiki/Botnet
http://es.wikipedia.org/wiki/Botnet
http://es.wikipedia.org/wiki/Bot
http://es.wikipedia.org/wiki/Borg

Funcionamiento

Como bien indica el gráfico, el primer objetivo es distribuir el malware suficiente para lograr la mayor cantidad de equipos infectados con el troyano -cliente que conecta a los usuarios con el/los botmaster/s responsable/s de la botnet-.

Esta distribución por supuesto se realiza mediante mensajes masivos como los que se pudo ver a mediados de enero y por la cual muchos usuarios son engañados[10]. Títulos como "la muerte de Fidel", "muertos en una tormenta que arrasa Europa", "Saddam Hussein vive" lamentablemente llaman suficientemente la atención como para que miles de equipos sean infectados y comiencen a servir de base para nuevas olas de ataques.

Una vez que la red ha sido convenientemente armada (con 10 o miles de equipos), el botmaster (responsable) de la misma puede decidir con total libertad, remotamente y en cualquier parte del mundo qué hacer con la misma pudiendo, por ejemplo:

- Enviar spam
- Realizar ataques de denegación de servicio distribuido
- Construir servidores para alojar software warez, cracks, seriales, etc
- Construir servidores web para alojar material pornográfico y pedofílico
- Construir servidores web para ataques de phishing
- Redes privadas de intercambio de material ilegal
- Sniffing de tráfico web para robo de datos confidenciales
- Distribución e instalación de nuevo malware
- Abuso de publicidad online como adsense
- Manipulación de juegos online

El control de la red puede llevarse a cabo de diversas maneras: puede controlarse la red totalmente o en forma segmentada por canales de IRC, depender de DNS gratuitos que aseguran su movimiento permanente, cifrar el canal para evitar su rastreo, identificación o intromisiones de otras personas ajenas a la red.

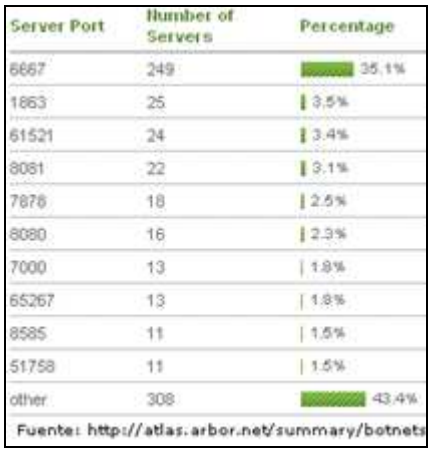
La forma más común de llevar este paso es obtener el control de uno o varios servidores IRC para enviar las ordenes de los demás nodos de la red. Este servidor denominado Comando y Control (C&C) es el

[10] El troyano "tormenta"
http://www.hispasec.com/unaaldia/3012/mediatico-troyano-tormenta-las-lecciones-aprend

punto más débil de la red, ya que si el mismo es identificado puede darse de baja, aislando al botmaster de su red.

Para solventar este problema, se han implementado redes P2P que permiten al botmaster cambiar de servidor a gusto, que el rastreo se dificulta e incluso, si la red es descubierta, la misma no podrá ser destruida en su totalidad por la alta redundancia de nodos. Estas redes aún se encuentran en un estadío de estudio y perfeccionamiento, por lo cual aún no son masivamente utilizadas, pero que sin duda marcan el futuro de las botnets.

En la siguiente estadística puede verse la gran utilización del puerto 6667 comúnmente utilizado para controlar a SDBot, uno de los malware más antiguos (junto a Agobot, Spybot y GTBot) destinado a construir botnets. Esto demuestra el amplio uso de estas redes y cómo las mismas pueden impactar en el uso globalizado de Internet.



Server Port	Number of Servers	Percentage
6667	249	35.1%
1863	25	3.5%
61521	24	3.4%
8081	22	3.1%
7878	18	2.5%
8080	16	2.3%
7000	13	1.8%
65267	13	1.8%
8585	11	1.5%
51758	11	1.5%
other	308	43.4%

Fuente: http://atlas.arbor.net/summary/botnets

Imagen 2 – Puertos Utilizados

Nota: *este puerto también es utilizado por otros programas de Chat legales. El gráfico muestra la totalidad, es decir considerando el tráfico de las botnets y el legal.*

También se ve otra evolución: debido al filtro del protocolo IRC implementado por las organizaciones, el envío de comandos de control se realiza por medio de HTTP o IM (mensajería instantánea), el cual generalmente no es filtrado debido al uso de Internet en esas empresas.

Si se analiza cualquiera del malware actual para la construcción de botnets puede encontrarse comandos como los siguientes[11]:

mac.login log in del usuario
ftp.execute actualización del bot a través de dirección ftp
...
http.execute actualización del bot a través de dirección http
rsl.logoff log out del usuario
rsl.shutdown apagar el equipo
rsl.reboot reiniciar el equipo
pctrl.kill terminar un proceso
...
ddos.httpflood ataque de denegación de servicios
ddos.synflood ataque de denegación de servicios
...
harvest.emailshttp obtiene lista de correos vía http
harvest.emails obtiene lista de correos

Como puede verse la lista de commandos involucra desde el login del botmaster, hasta el apagado del equipo, ataques DDoS, la actualización del bot, el envío de spam o cuanta actividad el creador del bot pueda imaginar.

El dinero (millones) en la red

Una vez que la red está perfectamente construida y controlada, sólo basta alquilarla o venderla al mejor postor. La persona que adquiera el "servicio" podrá utilizar la red para las actividades que desee y que ya se enumeraron.

A modo de ejemplo, un spammer podrá alquilar la red para enviar sus correos, una organización podría realizar publicidad en forma masiva, una empresa podría atacar a su competidor y sacar sus servicios web del aire, un pedófilo podría distribuir su material anónimamente…

[11] Comandos utilizados en botnets
http://www.lurhq.com/research_threat.html

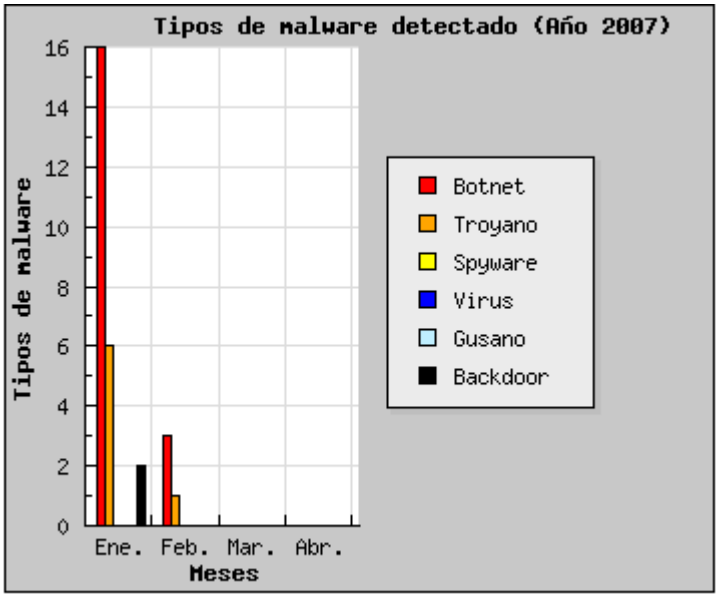
Como es fácil adivinar, toda la red de delincuentes involucrados se beneficia de esta red:

- El creador de malware vende su “producto/servicio” al creador de la botnet
- El botmaster alquila/vende la red
- El spammer distribuye más correo con publicidad
- Las empresas venden los productos publicitados
- Cualquiera de ellos distribuye más malware infectando más equipos y retroalimentando el sistema

Más números

En este caso en particular, lamentablemente las estadísticas manejan números muy dispares y sólo pueden confundir si los mismos son señalados por lo que es preferible no mencionar demasiado. Lo que es importante remarcar es que las cifras mencionadas por los distintos estudios pueden asustar.

A modo de ejemplo, y si bien la muestra no es representativa, se muestra el porcentaje de malware distribuido con el fin de crear botnets en 2007 y registrado por la UNAM-CERT[12].



Fuente: http://www.malware.unam.mx/ver_reportes2.dsc?idcatalogo=2

Otro aspecto que entrega una idea clara de la forma en que estas redes son controladas es observando el tráfico de correos electrónicos generados por los proveedores internacionales[13]. Puede observarse a Telefonica, Telecom, BellSouth y Fibertel en los primeros 50 puestos lo que indica a las claras que gran parte del correo enviado es generado desde los hogares de los usuarios gracias a la utilización de equipos zombies.

[12] Proyecto malware de UNAM-CERT (Universidad Nacional Autónoma de México-Equipo de Respuesta a Incidentes de Seguridad en Cómputo)
http://www.malware.unam.mx/ver_reportes2.dsc?idcatalogo=2

[13] Envío de correos por distintos proveedores
http://www.senderbase.org/search?page=domains

Un problema global creado por problemas individuales

El poder de una red distribuida es proporcional a la cantidad de usuarios conectados a la red y al poder individual que aporte cada nodo.

Así, como se menciona al comienzo del presente, los responsables del spam existente terminamos siendo los usuarios por falta de medidas de prevención adecuadas, que ayudarían a mitigar, en gran escala, este problema mundial de abuso de recursos ajenos.

Las redes descubiertas por los investigadores[14] no hacen más que confirmar el número alarmante que están alcanzando estas redes y sus objetivos delictivos.

La pregunta ¿en qué puede afectar que mi equipo sea infectado? pasó a ser fundamental, porque aquel usuario aislado, que sólo tenía acceso a sus recursos particulares y que no interactuaba con sus pares, está desapareciendo a favor de usuarios altamente conectados que interactúan en forma permanente con otros sistemas y que, como puede verse, es capaz de afectarlos directamente al formar parte de una botnet.

Por eso es fundamental tomar conciencia de este problema, que es global y depende de la educación (de la buena educación) de todos nosotros hacia nuestros pares. La protección y el uso responsable pasaron a ser una parte importante de un sistema informático.

[14] Estudio de Botnes
http://news.netcraft.com/archives/2004/09/08/botnet_with_10000_machines_shut_down
http://www.technewsworld.com/story/48174.html
http://www.honeynet.org/papers/bots/
http://www.cs.wisc.edu/~vinod/botnets.pdf